UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/531,431	03/13/2006	David Jeal	P08620US01/BAS	9093

881 7590 10/13/2010

STITES & HARBISON PLLC
1199 NORTH FAIRFAX STREET
SUITE 900
ALEXANDRIA, VA 22314

EXAMINER	
YU, HENRY W	
ART UNIT	PAPER NUMBER
2182	

NOTIFICATION DATE	DELIVERY MODE
10/13/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

iplaw@stites.com

Office Action Summary	Application No.	Applicant(s)	
	10/531,431	JEAL ET AL.	
	Examiner	Art Unit	
	HENRY YU	2182	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 July 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-66* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-66* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 November 2009* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

INFORMATION CONCERNING RESPONSES

Response to Amendment

1. This Office Action is in response to applicant's communication filed on July 29, 2010, in response to PTO Office Action mailed on January 29, 2010. The Applicant's remarks and amendments to the claims and/or the specification were considered with the results that follow.

2. In response to the last Office Action, no claims have been amended, cancelled, or added. As a result, **claims 1-66** are now pending in this application.

Response to Arguments

3. Applicant's arguments filed on July 29, 2010, in response to the office action mailed on January 29, 2010, have been fully considered but are not persuasive.

Applicant argues that Cronce et al. (Patent Number US 7,032,240 B1) does not disclose that the "*authentication storage means*" and the "*security data entry means*" are separate devices. However, further review of the claims and the office action dated on July 29, 2010, shows that there are two distinct components, which are the portable authorization device 140 and the physical direct information authority 160 (as seen in FIG. 1 of Cronce et al.). The physical direct information authority 160 is connected to the portable authorization device 140 through a direct message interface circuit 147, which may consist of a card reader and associated circuitry **[Column 8, line 67 to Column 9, lines 1-2]**. The Examiner was in no way asserting that the physical direct

information authority 160 is meant to represent the "*authentication storage means*" and the "*security data entry means.*" Furthermore, Examiner disagrees with the Applicant's argument that physical direct information authority 160 is connected "directly" to the portable authorization device 140 as it pertains to the claim passage "*security data entry means for obtaining security data independently of the data processing apparatus,*" with the data processing apparatus represented by the host computer of Cronce et al. The passage is interpreted by the Examiner as a security device must be connected through an intermediary device (represented by the portable authorization device 140) as opposed to being directly connected to a host device (as seen in FIG. 1 of Cronce et al.).

As for the argument stating that Cronce et al. does not disclose "*render the second coupling means [physically] available [or unavailable] for coupling to the data processing apparatus,*" Examiner notes that although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns,* 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The current claim language does not explicitly disclose the "*configuration means*" is a physical component similar to a connector cover (e.g. a cap). Instead, the "*configuration means*" can also apply to signaling/software means of rendering an interface available.

REJECTIONS BASED ON PRIOR ART

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. **Claims 1-2, 7-8, 16-18, 23-29, 33, 35, 38-39, 43, 48-54, 58, 60, and 63-64** are rejected under 35 U.S.C. 102(e) as being anticipated by Cronce et al. (Patent Number US 7,032,240 B1).

As per **claim 1**, Cronce et al. discloses "*a device* ***(the focus is on the portable authorization device 140)*** *for connection to a data processing apparatus* ***(host system 110)****, the device including first coupling means for operative coupling to authentication storage means* ***(physical direct information authority 160)*** *storing predetermined information relating to the authentication of a transaction with the data processing apparatus* ***(the physical direct information authority 160 includes a memory for storing the authorization information 171 and other data; Column 5, lines 55-59; Column 6, lines 54-58; FIG. 1 and 3)***," "*second coupling means for operative coupling to the data processing apparatus* ***(Column 5, lines 27-31; FIG. 1 and 3)****, the device when operatively coupled to the data processing apparatus being responsive to an authentication process carried out via a communications link for authenticating the transaction, the authentication process involving the use of the predetermined*

information ***(Column 7, lines 51-67; Column 8, lines 1-2; Column 8, lines 22-28)***," "*security data entry means for obtaining security data independently of the data processing apparatus* ***(particularly true for the direct information authority 160, which communicates directly with the portable authorization device 140; Column 6, lines 47-50; FIG. 1)***," and "*means for storing the security data temporarily* ***(note that data within the portable authorization device can be replaced or updated (implying that the data can indeed be temporary) (Column 6, lines 10-13), with the portable authorization device containing memory; FIG. 3)***."

As per **claim 2**, Cronce et al. discloses "*wherein the security data is stored temporarily by means of a transient power source* ***(since the portable authorization device does not have its own power source, it must rely on another source (in this case from the host system) in order to operate its internal circuitry (which includes memory with a focus on the RAM as seen in FIG. 3); Column 14, lines 49-51)***."

As per **claim 7**, Cronce et al. discloses "*means for analysing the entered security data for determining whether to allow access to the predetermined information* ***(Column 3, lines 56-59)***."

As per **claim 8**, Cronce et al. discloses "*a device for connection to a data processing apparatus, the device including first coupling means for operative coupling to authentication storage means storing predetermined information relating to the authentication of a transaction with the data processing apparatus* ***(the physical direct information authority 160 includes a memory for storing the authorization***

information 171 and other data; Column 5, lines 55-59; Column 6, lines 54-58; FIG. 1 and 3)," "*second coupling means for operative coupling to the data processing apparatus* ***(Column 5, lines 27-31; FIG. 1 and 3)***," "*the device when operatively coupled to the data processing apparatus being responsive to an authentication process carded out via a communications link for authenticating the transaction, the authentication process involving the use of the predetermined information and configuration means for selectively rendering the second coupling means available for coupling to the data processing apparatus* ***(Column 7, lines 51-67; Column 8, lines 1-2; Column 8, lines 22-28)***."

As per **claim 16**, Cronce et al. discloses "*security data entry means for obtaining security data independently of the data processing apparatus* ***(particularly true for the direct information authority 160, which communicates directly with the portable authorization device 140; Column 6, lines 47-50)****, and means for analysing the entered security data for determining whether to allow access to the predetermined information* ***(Column 3, lines 56-59)***."

As per **claim 17**, Cronce et al. discloses "*security data entry means for obtaining security data independently of the data processing apparatus* ***(particularly true for the direct information authority 160, which communicates directly with the portable authorization device 140; Column 6, lines 47-50)***" and "*means for storing the security data temporarily* ***(note that data within the portable authorization device can be replaced or updated (implying that the data can indeed be temporary) (Column 6, lines 10-13), with the portable authorization device containing memory; FIG. 3)***."

As per **claims 18 and 43**, Cronce et al. discloses "*the device controls access to the predetermined information* ***(Column 3, lines 56-59)***." **Claim 43** discloses the same limitation as **claim 18**, and is hence rejected accordingly.

As per **claims 23 and 48**, Cronce et al. discloses "*a data processing module for controlling the communication with the data processing apparatus* ***(through the processing unit 141 in conjunction the host system interface circuit 145; FIG. 3)***." **Claim 48** discloses the same limitation as **claim 23**, and is hence rejected accordingly.

As per **claims 24 and 49**, Cronce et al. discloses "*the data processing module of the device is configured for communicating with a corresponding data processing module of the data processing apparatus* ***(through the processing unit 141 in conjunction the host system interface circuit 145 (with emphasis on the interface circuit)); FIG. 3)***." **Claim 49** discloses the same limitation as **claim 24**, and is hence rejected accordingly.

As per **claims 25 and 50**, Cronce et al. discloses "*communication between the authentication storage means* ***(through the interface circuit 147)*** *and the data processing apparatus* ***(through the interface circuit 145)*** *is performed via the respective data processing modules* ***(in conjunction with the processing unit 141; FIG. 3)***." **Claim 50** discloses the same limitation as **claim 25**, and is hence rejected accordingly.

As per **claims 26 and 51**, Cronce et al. discloses the use of encryption and decryption as disclosed in the limitation "*the data processing module of the device includes means for decrypting encrypted data received from the data processing*

module of the data processing apparatus ***(note that the system of Cronce et al. has the ability to decrypt encrypted transferred data; Column 16, lines 34-35)***." **Claim 51** discloses the same limitation as **claim 26**, and is hence rejected accordingly.

As per **claims 27 and 52**, Cronce et al. discloses the use of encryption and decryption as disclosed in the limitation "*the data processing module of the device includes means for encrypting data transmitted to the data processing module of the data processing apparatus* ***(Column 16, lines 18-21)***." **Claim 52** discloses the same limitation as **claim 27**, and is hence rejected accordingly.

As per **claims 28 and 53**, Cronce et al. discloses the use of encryption and decryption as disclosed in the limitation "*the data processing modules of the device comprise a key for allowing decryption of data* ***(Column 10, lines 16-19)***." **Claim 53** discloses the same limitation as **claim 28**, and is hence rejected accordingly.

As per **claims 29 and 54**, Cronce et al. discloses the use of encryption and decryption as disclosed in the limitation "*the key comprises a shared secret key for each of the respective data processing modules* ***(one encryption algorithm used is public key algorithm; Column 10, lines 16-19)***." **Claim 54** discloses the same limitation as **claim 29**, and is hence rejected accordingly.

As per **claims 33 and 58**, Cronce et al. discloses "*the transaction is a transaction involving use of data processing functions of the data processing apparatus* ***(Column 3, lines 56-59)***." **Claim 58** discloses the same limitation as **claim 33**, and is hence rejected accordingly.

As per **claims 35 and 60**, Cronce et al. discloses "*the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information* ***(steps 224 to 228; FIG. 10)***." **Claim 60** discloses the same limitation as **claim 35**, and is hence rejected accordingly.

As per **claims 38 and 63**, Cronce et al. discloses "*in combination with the data processing apparatus* ***(as seen in FIG. 1 and 3)***." **Claim 63** discloses the same limitation as **claim 38**, and is hence rejected accordingly.

As per **claims 39 and 64**, Cronce et al. discloses "*in combination with the telecommunications system* ***(network such as the Internet; Column 7, lines 43-46)***." **Claim 64** discloses the same limitation as **claim 39**, and is hence rejected accordingly.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 21, 30-32, 34, 36, 40-42, 46, 55-57, 59, 61, and 65-66** are rejected under 35 U.S.C. 103(a) as being unpatentable over Cronce et al. (Patent Number US 7,032,240 B1) in view of Dosch (Publication Number US 2002/0069364 A1).

As per **claims 21 and 46**, Cronce et al. discloses "*the device*" (*see rejection to* ***claim 1*** *above*). However, Cronce et al. does not explicitly disclose the use of PIN

stored on a authentication storage means as disclosed in the limitation "*the security data comprise a Personal Identification Number (PIN) and analysing means compares the PIN obtained by the security data means with a PIN stored on the authentication storage means and only allows access to the predetermined information when the respective PINs match.*"

Dosch discloses "*the security data comprise a Personal Identification Number (PIN) and analysing means compares the PIN obtained by the security data means with a PIN stored on the authentication storage means and only allows access to the predetermined information when the respective PINs match* ***(while the identification module 15 contains a PIN, the focus is on an encoded authorization code which is matched with the internet terminal 11 (indicating the presence of an analyzing means). The encoded authorization code prevents or makes difficult the use of imitated or unauthorized identification modules; Page 2, paragraph 0027)***." It would have been obvious to one of ordinary skill in the art to combine the device of Cronce et al. with elements of Dosch as both prior arts of record are in the same field of device authorization and security, particularly through the use of external devices. Furthermore, Dosch notes that by enabling the ability to remove an identification module, unauthorized or undesired access by third parties is prevented **[Page 2, paragraph 0014]**. Furthermore, further security is added in that imitation of an identification module is rendered very difficult by an authorization code which is matched to an apparatus (e.g. in a form of a PIN on the identification module) **[Page 2,**

paragraph 0015]. **Claim 46** discloses the same limitation as **claim 21**, and is hence rejected accordingly.

As per **claims 30 and 55**, Cronce et al. discloses "*the device*" (*see rejection to* ***claim 1*** *above*). However, Cronce et al. does not explicitly disclose "*the device is operatively coupleable to one of more of a plurality of said authentication storage means, each of which is registerable with a common telecommunication system, and wherein the authentication process is performed by a communications link with the telecommunications system.*"

Dosch discloses "*the device is operatively coupleable to one of more of a plurality of said authentication storage means* ***(identification module 15)****, each of which is registerable with a common telecommunication system, and wherein the authentication process is performed by a communications link with the telecommunications system* ***(Page 3, paragraph 0029)***."

It would have been obvious to one of ordinary skill in the art to combine the device of Cronce et al. with elements of Dosch as both prior arts of record are in the same field of device authorization and security, particularly through the use of external devices (*see* ***claim 21*** *for further motivations to combine*). **Claim 55** discloses the same limitation as **claim 30**, and is hence rejected accordingly.

As per **claims 31 and 56**, the combination of Cronce et al. and Dosch discloses "*the device*" (*see rejection to* ***claim 30*** *above*). Dosch further discloses "*the predetermined authentication information stored by each authentication storage means corresponds to information which is used to authenticate a user of that authentication*

storage means in relation to the telecommunications system ***(Page 3, paragraphs 0028-0029)***." **Claim 56** discloses the same limitation as **claim 31**, and is hence rejected accordingly.

As per **claims 32 and 57**, the combination of Cronce et al. and Dosch discloses "*the device*" (*see rejection to* ***claim 30*** *above*). Dosch further discloses "*each user is authenticated in the telecommunications system by means of the use of a smart card or subscriber identity module* ***(the system of Dosch relates to an identification module utilizing SIM for use with an internet terminal, with the internet terminal capable of mobile communications; Page 1, paragraph 0001)****, and in which the authentication storage means respective to that user corresponds to or simulates the smart card for that user* ***(Page 3, paragraph 0028)***." **Claim 57** discloses the same limitation as **claim 32**, and is hence rejected accordingly.

As per **claims 34 and 59**, Cronce et al. discloses "*the device*" (*see rejection to* ***claim 1*** *above*). However, Cronce et al. does not explicitly disclose "*the authentication storage means is specific to that device.*"

Dosch discloses "*the authentication storage means is specific to that device* ***(the identification module 15 contains an encoded authorization code which prevents or makes difficult the use of imitated or unauthorized identification modules; Page 2, paragraph 0027)***."

It would have been obvious to one of ordinary skill in the art to combine the device of Cronce et al. with elements of Dosch as both prior arts of record are in the same field of device authorization and security, particularly through the use of external

devices (*see **claim 21** for further motivations to combine*). **Claim 59** discloses the same limitation as **claim 34**, and is hence rejected accordingly.

As per **claims 36 and 61**, the combination of Cronce et al. and Dosch discloses "*the device*" (*see rejection to **claim 30** above*). Dosch further discloses "*the telecommunications system includes means for levying a charge for the transaction when authorised **(access subject to costs may be charged for the duration of the access; Page 3, paragraph 0035)***." **Claim 61** discloses the same limitation as **claim 36**, and is hence rejected accordingly.

As per **claims 40 and 65**, Cronce et al. discloses "*the device*" (*see rejection to **claim 1** above*). However, Cronce et al. does not explicitly disclose wireless communication as disclosed in the limitation "*the authentication storage means communicates wirelessly to authenticate the transaction.*"

Dosch explicitly discloses the use of wireless communication as "*the authentication storage means communicates wirelessly to authenticate the transaction **(the identification module 15 may be designed as a contactless transponder through such means as radio-frequency identification; Page 2, paragraph 0024)***."

It would have been obvious to one of ordinary skill in the art to combine the device of Cronce et al. with elements of Dosch as both prior arts of record are in the same field of device authorization and security, particularly through the use of external devices (*see **claim 21** for further motivations to combine*). **Claim 65** discloses the same limitation as **claim 40**, and is hence rejected accordingly.

As per **claims 41 and 66**, Cronce et al. discloses "*the device*" (*see rejection to* ***claim 1*** *above*). However, Cronce et al. does not explicitly disclose the use of SIM cards as disclosed in the limitation "*the authentication storage means comprises a subscriber identity module which authenticates the transaction when the subscriber identity module is operable in a mobile terminal.*"

Dosch discloses "*the authentication storage means comprises a subscriber identity module which authenticates the transaction when the subscriber identity module is operable in a mobile terminal* ***(the system of Dosch relates to an identification module utilizing SIM for use with an internet terminal, with the internet terminal capable of mobile communications; Page 1, paragraph 0001)***."

It would have been obvious to one of ordinary skill in the art to combine the device of Cronce et al. with elements of Dosch as both prior arts of record are in the same field of device authorization and security, particularly through the use of external devices (*see* ***claim 21*** *for further motivations to combine*). **Claim 66** discloses the same limitation as **claim 41**, and is hence rejected accordingly.

As per **claim 42**, the combination of Cronce et al. and Dosch discloses "*the device*" (*see rejection to* ***claim 30*** *above*). Dosch further discloses "*the authentication storage means comprises a subscriber identity module which is further operable to authenticate a mobile terminal for use in the system* ***(the system of Dosch relates to an identification module utilizing SIM for use with an internet terminal, with the internet terminal capable of mobile communications; Page 1, paragraph 0001)***."

8. **Claims 3-6** are rejected under 35 U.S.C. 103(a) as being unpatentable over Cronce et al. (Patent Number US 7,032,240 B1) in view of Zhou et al. (Patent Number US 6,559,620 B2).

As per **claim 3**, while Cronce et al. discloses "*the device*" (*see rejection to* ***claim 2*** *above*), Zhou et al. discloses the use of piezo-electric means as disclosed in the limitation "*the transient power source comprises piezo electric means* ***(transducer 720, which can be a piezo-electric device; Column 7, line 35)***."

It would have been obvious to one of ordinary skill in the art to combine the device of Cronce et al. with piezo-electric elements as disclosed by Zhou et al. since in several situations it is difficult to ascertain the remaining amount of energy supply of an internal battery at a given time **[Column 1, lines 18-20]**. Utilizing an internal piezo-electric element for electrical charge can preclude not only having to periodically charge any internal batteries through an outside source, but also ensure the existence of electrical power even if an internal battery is drained as piezo-electric components generate electrical energy through mechanical means.

As per **claim 4**, Cronce et al. and Zhou et al. discloses "*the device*" (*see rejection to* ***claim 3*** *above*). Zhou et al. further discloses "*the piezo electric means comprises one or more piezo electric cells* ***(a piezo-electric device (note that the claim disclosed one 'or' more, and hence can be interpreted as the system can contain only one cell); Column 7, line 35)***."

As per **claim 5**, while Cronce et al. discloses "*the device*" (*see rejection to* ***claim 2*** *above*), Zhou et al. discloses the idea of a power source through an input means as

"*the transient power source is charged by the security data entry means* ***(the example shown has the piezo-electric based transducer having mechanical pressure exerted upon it is generate an electrical signal (Column 7, lines 42-47). It would have been obvious to equate the passage with a entry means utilizing piezo-electric components as such components produce electrical signals through mechanical (such as pressing a button) means)***."

It would have been obvious to one of ordinary skill in the art to combine the device of Cronce et al. with piezo-electric elements as disclosed by Zhou et al. since in several situations it is difficult to ascertain the remaining amount of energy supply of an internal battery at a given time **[Column 1, lines 18-20]**. Utilizing an internal piezo-electric element for electrical charge can preclude not only having to periodically charge any internal batteries through an outside source, but also ensure the existence of electrical power even if an internal battery is drained as piezo-electric components generate electrical energy through mechanical means.

As per **claim 6**, while Cronce et al. discloses "*the device*" (*see rejection to* ***claim 2*** *above*), Zhou et al. discloses "*the transient power source comprises a reehargeable battery* ***(Column 7, line 32)***."

It would have been obvious to one of ordinary skill in the art to combine the device of Cronce et al. with a rechargeable battery as disclosed by Zhou et al. in order to prevent a physical waste of batteries **[Column 1, line 21]**.

9. **Claims 9-15** are rejected under 35 U.S.C. 103(a) as being unpatentable over Cronce et al. (Patent Number US 7,032,240 B1) in view of Wang (Patent Number US 5,813,421).

As per **claim 9**, while Cronce et al. discloses "*the device*" (*see rejection to **claim 8** above*), Wang discloses "*the configuration means comprises means for selectively making the second coupling means available externally of the device housing **(through the use of a lipstick swivel mechanism that is designed to protrude out or to withdraw back into its housing by rotating operation of an enclosed object; Column 1, lines 10-12)***."

It would have been obvious to one of ordinary skill in the art to combine the device of Cronce et al. with a configuration means for selectively making a coupling means (or any object within a housing) available externally of a housing as disclosed by Wang in order to protect the coupling means (or any object within a housing) when not in use. Only when in use is the coupling means (or any object within a housing) made available externally of the housing.

As per **claim 10**, the combination of Cronce et al. and Wang discloses "*the device*" (*see rejection to **claim 9** above*). Wang further discloses "*the configuration means comprises a removable cap **(upper lid 21; FIG. 3A)***."

As per **claim 11**, the combination of Cronce et al. and Wang discloses "*the device*" (*see rejection to **claim 9** above*). Wang further discloses "*the configuration means comprises a closure member coupled to and moveable with respect to the housing for selectively closing an aperture in the housing **(Column 1, lines 12-27)***."

As per **claim 12**, the combination of Cronce et al. and Wang discloses "*the device*" (*see rejection to* ***claim 9*** *above*). Wang further discloses "*interconnection means for connecting the closure member and the second coupling means* ***(a screw-cup member 12 include a cup portion 12a for holding a bullet; Column 1, lines 19-20)****, the arrangement being such that, as the closure member is moved to open the aperture, the second coupling means emerges from the aperture* ***(Column 1, lines 19-27)***."

As per **claim 13**, while Cronce et al. discloses "*the device*" (*see rejection to* ***claim 8*** *above*), Wang discloses "*a knob mounted on the device housing for rotation with respect thereto* ***(a spiral-base member 15 that can be turned)****, and means for converting rotation of said knob into linear movement of the second coupling means such that rotation of said knob in a first direction causes the second coupling means to emerge from an aperture in the device housing* ***(when the spiral-base member 15 is turned, the bullet held by the cup portion is protruded)*** *and rotation of said knob in a second direction causes the second coupling means to be retracted through said aperture* ***(when the spiral-base member 15 is turned, the bullet held by the cup portion is withdrawn; Column 1, lines 19-30)***."

It would have been obvious to one of ordinary skill in the art to combine the device of Cronce et al. with a configuration means for selectively making a coupling means (or any object within a housing) available externally of a housing as disclosed by Wang in order to protect the coupling means (or any object within a housing) when not

in use. Only when in use is the coupling means (or any object within a housing) made available externally of the housing.

As per **claim 14**, the combination of Cronce et al. and Wang discloses "*the device*" (*see rejection to* ***claim 9*** *above*). Wang further discloses "*the device housing includes two parts* ***(screw-cup member 12 and a cup portion 12a for holding a bullet)*** *moveable with respect to one another between a first arrangement where the second coupling means is contained within the housing* ***(when the spiral-base member 15 is turned, the bullet held by the cup portion is protruded)*** *and a second arrangement where the second coupling means is exposed for connection to the data processing apparatus* ***(when the spiral-base member 15 is turned, the bullet held by the cup portion is withdrawn; Column 1, lines 19-30)***."

As per **claim 15**, the combination of Cronce et al. and Wang discloses "*the device*" (*see rejection to* ***claim 9*** *above*). Wang further discloses "*the two parts are pivotally coupled together* ***(the cup portion 12a is integrally formed with a screw portion 12b; Column 1, lines 20-22)***."

10. **Claims 19-20, 22, 37, 44-45, and 47** are rejected under 35 U.S.C. 103(a) as being unpatentable over Cronce et al. (Patent Number US 7,032,240 B1) in view of Gregory et al. (Patent Number US 7,266,849 B1).

As per **claims 19 and 44**, while Cronce et al. discloses "*the device*" (*see rejection to* ***claim 1*** *above*), Gregory et al. discloses "*the security data entry means comprises alphanumeric data entry means* ***(before the system is enabled (in this***

embodiment a washing machine), a sequence of pushbutton depressions or keypad (emphasis) depressions must be implemented; Column 3, lines 54-60)."

It would have been obvious to one of ordinary skill in the art to combine the device of Cronce et al. with a security entry means comprising an alphanumeric data entry means as disclosed by Gregory et al. as a means of deterring unauthorized use of electronic devices **[Column 1 lines 6-7]**, where in this case a correct code must be manually entered. **Claim 44** discloses the same limitation as **claim 19**, and is hence rejected accordingly.

As per **claims 20 and 45**, while Cronce et al. discloses "*the device*" (*see rejection to **claim 1** above*), Gregory et al. discloses "*the security data entry means comprises a keypad **(before the system is enabled (in this embodiment a washing machine), a sequence of pushbutton depressions or keypad (emphasis) depressions must be implemented; Column 3, lines 54-60)***."

It would have been obvious to one of ordinary skill in the art to combine the device of Cronce et al. with a security entry means comprising a keypad as disclosed by Gregory et al. as a means of deterring unauthorized use of electronic devices **[Column 1 lines 6-7]**, where in this case a correct code must be manually entered. **Claim 45** discloses the same limitation as **claim 20**, and is hence rejected accordingly.

As per **claims 22 and 47**, while Cronce et al. discloses "*the device*" (*see rejection to **claim 1** above*), Gregory et al. discloses "*a display for displaying security information **(display 36 such as an LED array; Column 3, lines 37)***."

It would have been obvious to one of ordinary skill in the art to combine the device of Cronce et al. with a security entry means comprising a keypad as disclosed by Gregory et al. as a means of deterring unauthorized use of electronic devices **[Column 1 lines 6-7]**, where the device can display the necessary procedures that the user must go through to use the device. **Claim 47** discloses the same limitation as **claim 22**, and is hence rejected accordingly.

As per **claim 37**, while Cronce et al. discloses "*the device*" (*see rejection to **claim 1** above*), Gregory et al. discloses "*the security data entry means comprises a rotary knob **(before the system is enabled (in this embodiment a washing machine), a sequence of control knob (emphasis) settings must be implemented; Column 3, lines 54-60)***."

It would have been obvious to one of ordinary skill in the art to combine the device of Cronce et al. with a security entry means comprising a knob as disclosed by Gregory et al. as a means of deterring unauthorized use of electronic devices **[Column 1 lines 6-7]**, where in this case a correct code must be manually entered.

CLOSING COMMENTS

Conclusions

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to HENRY YU whose telephone number is (571)272-9779. The examiner can normally be reached on Monday to Friday, 8:00 AM to 5:30 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, TARIQ HAFIZ can be reached on (571) 272-6729. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/H. Y./
Examiner, Art Unit 2182
October 1, 2010

/Tariq Hafiz/
Supervisory Patent Examiner, Art Unit 2182